

# INTERNATIONAL SEARCH REPORT

Int'l. Application No  
PCT/JP2004/018988

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/044018 A1 (TOMLINSON DAVID ROBIN) 6 March 2003 (2003-03-06) abstract paragraph '0006! – paragraph '0008!	1-27
A	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography" 1997, CRC PRESS LLC, USA, XP002318652 page 490 page 498 – page 499 page 544 page 546 page 551 – page 553 page 578 – page 581	1-27
A	EP 1 241 826 A (HITACHI, LTD) 18 September 2002 (2002-09-18) abstract	1-27

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

### \* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*&\* document member of the same patent family

Date of the actual completion of the international search

22 February 2005

Date of mailing of the international search report

12/04/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

San Millán Maeso, J

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

Interr Application No  
PCT/JP2004/018988

Patent document cited in search report	Publication date		Patent family member(s)	Publication date
US 2003044018	A1	06-03-2003	GB 2378539 A EP 1423765 A2 WO 03021400 A2	12-02-2003 02-06-2004 13-03-2003
EP 1241826	A	18-09-2002	JP 2002271312 A EP 1241826 A2 US 2002131601 A1	20-09-2002 18-09-2002 19-09-2002